



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: Rajaniemi, Jaakko

Serial No. TO BE ASSIGNED

Corresponding to PCT/EP98/08064, filed 10 December 1998

Filed: July 28, 2000

Docket No.: 975.311USW1

Title: A METHOD FOR A SECURE DETACH PROCEDURE IN A RADIO
TELECOMMUNICATION NETWORK

CERTIFICATE UNDER 37 C.F.R. 1.10:

'Express Mail' mailing number: EL492431597US

Date of Deposit: July 28, 2000

The undersigned hereby certifies that this Transmittal Letter and the paper or fee, as described herein, are being deposited with the United States Postal Service 'Express Mail Post Office To Addressee' service under 37 CFR 1.10 and is addressed to the Assistant Commissioner for Patents, Washington, D.C. 20231

By: Missy Lange

Missy Lange

Box Patent Application
Assistant Commissioner for Patents
Washington, D.C. 20231

REQUEST FOR CONTINUATION OF AN INTERNATIONAL APPLICATION
UNDER 37 C.F.R. §1.53(b)

This is a request for filing a continuation application under 37 C.F.R. §1.53(b) of prior pending international application number PCT/EP98/08064 filed on 10 December 1998 entitled A METHOD FOR A SECURE DETACH PROCEDURE IN A RADIO TELECOMMUNICATION NETWORK, which designated the United States.

1. ☒ Enclosed is a patent application containing 14 pages of specification, 4 pages of claims and 3 sheet(s) of drawings.
2. ☒ A preliminary amendment is enclosed.
3. ☒ Please amend the specification by inserting the following paragraph after the title:

This application is a continuation of international application serial number
PCT/EP98/08064, filed 10 December 1998.

4. ☐ Small entity status
 - a. ☐ A small entity statement is enclosed.
 - b. ☐ A small entity statement was filed in the prior non provisional application.
 - c. ☐ is no longer claimed.

The filing fee is calculated below

CLAIMS				
	Number Filed	Number Extra	Rate	Fee
Total Claims	21	1	X \$18.00	\$ 18.00
Indep. Claims	2		X \$78.00	\$
Multiply Dependent Claims				\$
Basic Fee				\$ 690.00
TOTAL				\$ 708.00

5. ☒ Payment of filing fees
☐ A check in the amount of _____ is enclosed.
☐ Please charge Deposit Account Number 50-1038.
☒ Is deferred.
6. ☒ The Commissioner is hereby authorized to credit any overpayment or charge any fees required under 37 C.F.R. §1.16-1.18 to Deposit Account Number 50-1038.
7. ☒ The priority of International application number PCT/EP98/08064, filed 10 December 1998, is claimed under 35 U.S.C. §120.
☐ A certified copy of the priority application is enclosed.
8. ☒ An UNSIGNED Declaration is enclosed.
9. ☐ An assignment of the invention to _____, Recordation Form Cover Sheet (Patents Only) and a check in the amount of \$40.
10. ☐ An Information Disclosure Statement, Form PTO 1449 and copies of _____ citations are enclosed.
11. ☒ Correspondence Address
- Altera Law Group
10749 Bren Road East
Minneapolis, Minnesota 55343
12. ☒ Address all correspondence to Michael B. Lasky.
13. ☒ Also enclosed: abstract
14. ☒ A return postcard is enclosed.

Respectfully submitted,

Altera Law Group, LLC
10749 Bren Road East, Opus 2
Minneapolis, MN 55343
(952) 912-0527

Date: July 28, 2000

By: _____

Michael B. Lasky
Reg. No. 29,555
MBL/jsc

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Rajaniemi, Jaakko	Examiner:	UNKNOWN
Serial No.:	TO BE ASSIGNED	Group Art Unit:	TO BE ASSIGNED
Filed:	July 28, 2000	Docket No.:	975.311USW1
Title:	A METHOD FOR A SECURE DETACH PROCEDURE IN A RADIO TELECOMMUNICATION NETWORK		

CERTIFICATE UNDER 37 C.F.R. 1.10:

'Express Mail' mailing number: EL492431597US

Date of Deposit: July 28, 2000

The undersigned hereby certifies that this Transmittal Letter and the paper or fee, as described herein, are being deposited with the United States Postal Service 'Express Mail Post Office To Addressee' service under 37 CFR 1.10 and is addressed to the Assistant Commissioner for Patents, Washington, D.C. 20231

By: 

Missy Lange

PRELIMINARY AMENDMENT

Box Patent Application
Assistant Commissioner for Patents
Washington, D.C. 20231

Dear Sir:

Please enter the following preliminary amendment into the above-referenced application.

ABSTRACT

Please insert the attached abstract into the application as the last page thereof.

CLAIMS

Please amend the claims as follows:

In claim 19, line 2, please replace "according to any of claims 1 to 18" with
-- according to claim 1 --.

In claim 20, line 2, please replace "according to any of claims 1 to 18" with

-- according to claim 1 --.

In claim 21, line 4, please replace "according to any of claims 1 to 18" with
-- according to claim 1 --.

REMARKS

The above preliminary amendment is made to insert an abstract page into the application and to remove multiple dependencies from the following claims: 19,20 and 21.

Applicant respectfully requests that this preliminary amendment be entered into the record prior to calculation of the filing fee and prior to examination and consideration of the above-identified application.

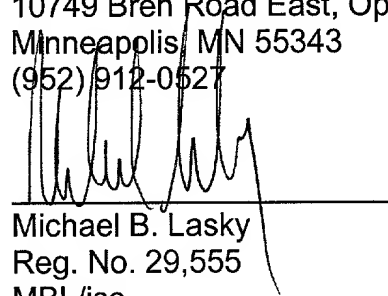
If a telephone conference would be helpful in resolving any issues concerning this communication, please contact Applicant's attorney of record, Michael B. Lasky at 952-912-0527.

Respectfully submitted,

Altera Law Group, LLC
10749 Bren Road East, Opus 2
Minneapolis, MN 55343
(952) 912-0527

Date: July 28, 2000

By:



Michael B. Lasky
Reg. No. 29,555
MBL/jsc

0022014322960

A METHOD FOR A SECURE DETACH PROCEDURE
IN A RADIO TELECOMMUNICATION NETWORK

5 FIELD OF THE INVENTION

The present invention relates to a method for performing a secure detach procedure in a radio telecommunication network, in particular in a so-called third generation
10 network. Moreover, the present invention relates to a corresponding registration procedure for registering a subscriber to such a telecommunication network. Also, the present invention relates to corresponding devices of subscriber terminals and network controlling devices which
15 are adapted to carry out these methods, and to a correspondingly adapted telecommunication network.

BACKGROUND OF THE INVENTION

20 In hitherto known telecommunication networks, a subscriber terminal as a first type radio transceiver device (hereinafter: mobile station MS), in order to be operated within a network, needs to be registered to the network NW, i.e. to a network controlling device like for example a
25 mobile services switching center MSC (or an SGSN), which controls so called base station controllers BSC, which in turn control base stations BS as second type radio transceiver devices.

30 To this end, each subscriber has a subscriber identity module SIM to be inserted into the used mobile station MS as a respective terminal equipment. The SIM contains a pre-stored international mobile subscriber identity number IMSI, by which a user can be identified. However, in order
35 to protect the user against being identified by an intruder

in the network, each user is assigned a temporary mobile subscriber identity TMSI. This identification which changes either from time to time or from area to area (when combined with a location area identifier LAI) allows an
5 "anonymous" identification of the user when using his terminal.

For details of the roughly described registration procedure including ciphering of transmitted data for authentication
10 at registration, which details are considered to be not necessarily to be described here, the reader is referred to the plurality of respective publicly available GSM specifications.

15 Likewise, an attached or registered subscriber or mobile station, respectively, will have to perform a detach from the network under specific conditions. For example, the mobile station will be detached from the network and its registration will be abandoned, in case the SIM module is
20 detached from the terminal equipment or the like.

In such cases, the mobile station MS sends a detach message to the network NW, the so-called IMSI DETACH INDICATION message. Upon receipt of the IMSI DETACH INDICATION the
25 network controlling device (MSC) sets an inactive indication for the mobile station MS, while no response is returned to the mobile station itself. (For details, also in this context it is referred to the respective GSM specifications). Namely, no authentication is conducted at
30 detach, when the mobile station initiating the detach procedure leaves the network.

Thus, there exists a possibility that a malicious user may obstruct or even terminate a third party's call by sending
35 detach messages with random identities of mobile stations

(i.e. random numbers of TMSI identifiers). Stated in other words, although it is not possible to interrupt the connection to a specific mobile station MS of a certain specified user by sending such a detach message, a lot of damage and irritation can be caused to a great number of users as well as to the operator of the network NW, when arbitrary calls and/or radio connections are blocked and/or terminated by the intention of a malicious third party.

10 A previously proposed approach to prevent this resides in performing an authentication procedure when a mobile station MS is to be detached from the network NW, i.e. upon receipt of a detach message at the network from the mobile station.

15 However, such a proposed authentication at detach is rather time consuming in many situations and has therefore only a limited applicability.

20 Moreover, performing an authentication procedure may not be feasible if the mobile station is performing power off, i.e. is switched off, or the available battery power is too low so that normal operation of the mobile station can not be assured any longer.

25

SUMMARY OF THE INVENTION

Hence, it is an object of the present invention to provide a simple and useful method for performing a detach from and/or a corresponding method for registration to a network, which prevent the above described problems.

30 According to the present invention, this object is achieved by a method for performing a detach of a terminal registered to a telecommunication network by

35

30 In particular, the proposed method enables an immediate authentication of the mobile station requesting a detach procedure upon receipt of the detach request message or the detach request, respectively. This authentication procedure is not time consuming and also applicable in case of a
35 mobile station being switched off (entering the power off

5

10

BRIEF DESCRIPTION OF THE DRAWINGS

15

Fig. 1 shows a flowchart of the registration procedure according to the present invention;

20

25

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

30

35

dependent on the specific situation, a location update request to the network NW. A request as such (to be valid for being evaluated) may be composed of more than one transmitted messages.

5

The network NW, which for the present description is assumed to be represented by the network controlling device as for example an MSC, in turn associates an identification to the mobile station MS. Associating such an

10 identification may be achieved in that the network NW allocates an identification to the terminal MS

The identification may be represented by the temporary mobile subscriber identity TMSI. Alternatively, as the
15 identification also the international mobile subscriber identity IMSI could be used. In general, any suitable identification may be used for identifying a respective mobile terminal MS, and the present invention is not restricted to the use of the TMSI or the IMSI as
20 identifications.

Additionally, the network NW allocates a signature (e.g. TMSI signature TMSI_SIG) corresponding to the identification and derived therefor on the basis of, for example, a coding algorithm like an algorithm known as the "Pretty Good Privacy" (PGP) algorithm, to the terminal, i.e. the mobile station MS. However, the deriving of the signature for and/or of the identification is not limited to the network side. Namely, alternatively, also the terminal MS may derive a signature for the identification by way of calculation. In this connection, information as to which algorithm for calculating the signature is to be chosen is in such a case exchanged between the network NW and the terminal MS. After having thus derived the

1. **Introduction**
 2. **Background**
 3. **Methodology**
 4. **Results**
 5. **Discussion**
 6. **Conclusion**
 7. **References**
 8. **Appendix**
 9. **Notes**
 10. **Tables**
 11. **Figures**
 12. **Supplementary Materials**
 13. **Correspondence**
 14. **Conflict of Interest**
 15. **Acknowledgments**
 16. **Author Contributions**
 17. **References**
 18. **Appendix**
 19. **Notes**
 20. **Tables**
 21. **Figures**
 22. **Supplementary Materials**
 23. **Correspondence**
 24. **Conflict of Interest**
 25. **Acknowledgments**
 26. **Author Contributions**
 27. **References**
 28. **Appendix**
 29. **Notes**
 30. **Tables**
 31. **Figures**
 32. **Supplementary Materials**
 33. **Correspondence**
 34. **Conflict of Interest**
 35. **Acknowledgments**
 36. **Author Contributions**
 37. **References**
 38. **Appendix**
 39. **Notes**
 40. **Tables**
 41. **Figures**
 42. **Supplementary Materials**
 43. **Correspondence**
 44. **Conflict of Interest**
 45. **Acknowledgments**
 46. **Author Contributions**
 47. **References**
 48. **Appendix**
 49. **Notes**
 50. **Tables**
 51. **Figures**
 52. **Supplementary Materials**
 53. **Correspondence**
 54. **Conflict of Interest**
 55. **Acknowledgments**
 56. **Author Contributions**
 57. **References**
 58. **Appendix**
 59. **Notes**
 60. **Tables**
 61. **Figures**
 62. **Supplementary Materials**
 63. **Correspondence**
 64. **Conflict of Interest**
 65. **Acknowledgments**
 66. **Author Contributions**
 67. **References**
 68. **Appendix**
 69. **Notes**
 70. **Tables**
 71. **Figures**
 72. **Supplementary Materials**
 73. **Correspondence**
 74. **Conflict of Interest**
 75. **Acknowledgments**
 76. **Author Contributions**
 77. **References**
 78. **Appendix**
 79. **Notes**
 80. **Tables**
 81. **Figures**
 82. **Supplementary Materials**
 83. **Correspondence**
 84. **Conflict of Interest**
 85. **Acknowledgments**
 86. **Author Contributions**
 87. **References**
 88. **Appendix**
 89. **Notes**
 90. **Tables**
 91. **Figures**
 92. **Supplementary Materials**
 93. **Correspondence**
 94. **Conflict of Interest**
 95. **Acknowledgments**
 96. **Author Contributions**
 97. **References**
 98. **Appendix**
 99. **Notes**
 100. **Tables**
 101. **Figures**
 102. **Supplementary Materials**
 103. **Correspondence**
 104. **Conflict of Interest**
 105. **Acknowledgments**
 106. **Author Contributions**
 107. **References**
 108. **Appendix**
 109. **Notes**
 110. **Tables**
 111. **Figures**
 112. **Supplementary Materials**
 113. **Correspondence**
 114. **Conflict of Interest**
 115. **Acknowledgments**
 116. **Author Contributions**
 117. **References**
 118. **Appendix**
 119. **Notes**
 120. **Tables**
 121. **Figures**
 122. **Supplementary Materials**
 123. **Correspondence**
 124. **Conflict of Interest**
 125. **Acknowledgments**
 126. **Author Contributions**
 127. **References**
 128. **Appendix**
 129. **Notes**
 130. **Tables**
 131. **Figures**
 132. **Supplementary Materials**
 133. **Correspondence**
 134. **Conflict of Interest**
 135. **Acknowledgments**
 136. **Author Contributions**
 137. **References**
 138. **Appendix**
 139. **Notes**
 140. **Tables**
 141. **Figures**
 142. **Supplementary Materials**
 143. **Correspondence**
 144. **Conflict of Interest**
 145. **Acknowledgments**
 146. **Author Contributions**
 147. **References**
 148. **Appendix**
 149. **Notes**
 150. **Tables**
 151. **Figures**
 152. **Supplementary Materials**
 153. **Correspondence**
 154. **Conflict of Interest**
 155. **Acknowledgments**
 156. **Author Contributions**
 157. **References**
 158. **Appendix**
 159. **Notes**
 160. **Tables**
 161. **Figures**
 162. **Supplementary Materials**
 163. **Correspondence**
 164. **Conflict of Interest**
 165. **Acknowledgments**
 166. **Author Contributions**
 167. **References**
 168. **Appendix**
 169. **Notes**
 170. **Tables**
 171. **Figures**
 172. **Supplementary Materials**
 173. **Correspondence**
 174. **Conflict of Interest**
 175. **Acknowledgments**
 176. **Author Contributions**
 177. **References**
 178. **Appendix**
 179. **Notes**
 180. **Tables**
 181. **Figures**
 182. **Supplementary Materials**
 183. **Correspondence**
 184. **Conflict of Interest**
 185. **Acknowledgments**
 186. **Author Contributions**
 187. **References**
 188. **Appendix**
 189. **Notes**
 190. **Tables**
 191. **Figures**
 192. **Supplementary Materials**
 193. **Correspondence**
 194. **Conflict of Interest**
 195. **Acknowledgments**
 196. **Author Contributions**
 197. **References**
 198. **Appendix**
 199. **Notes**
 200. **Tables**
 201. **Figures**
 202. **Supplementary Materials**
 203. **Correspondence**
 204. **Conflict of Interest**
 205. **Acknowledgments**
 206. **Author Contributions**
 207. **References**
 208. **Appendix**
 209. **Notes**
 210. **Tables**
 211. **Figures**
 212. **Supplementary Materials**
 213. **Correspondence**
 214. **Conflict of Interest**
 215. **Acknowledgments**
 216. **Author Contributions**
 217. **References**
 218. **Appendix**
 219. **Notes**
 220. **Tables**
 221. **Figures**
 222. **Supplementary Materials**
 223. **Correspondence**
 224. **Conflict of Interest**
 225. **Acknowledgments**
 226. **Author Contributions**
 227. **References**
 228. **Appendix**
 229. **Notes**
 230. **Tables**
 231. **Figures**
 232. **Supplementary Materials**
 233. **Correspondence**
 234. **Conflict of Interest**
 235. **Acknowledgments**
 236. **Author Contributions**
 237. **References**
 238. **Appendix**
 239. **Notes**
 240. **Tables**
 241. **Figures**
 242. **Supplementary Materials**
 243. **Correspondence**
 244. **Conflict of Interest**
 245. **Acknowledgments**
 246. **Author Contributions**

signature, the deriving side (i.e. NW or MS) informs the other side of the derived signature.

Both data items, the identification TMSI as well as the
5 identification signature TMSI_SIG are allocated to the mobile station MS in a secure mode, so that it is impossible for any other mobile station or any other third party to know the pair of these data items TMSI, TMSI_SIG. Of course, if in the above mentioned example case the
10 terminal MS derives the signature, the derived signature is informed to the network NW in a secure mode, to be securely associated to the identification, so that it is impossible for any other mobile station or any other third party to know the pair of these data items TMSI, TMSI_SIG.

15 In particular, according to the present invention, the network NW or the network controlling device MSC, respectively, associates and/or allocates also a signature TMSI_SIG in combination with the identifier TMSI itself to
20 the mobile station MS. Moreover, according to the present invention, the associated signature is used together with the identifier in a detach procedure, as described below.

Namely, in case the mobile station MS leaves the network NW
25 and is to be detached therefrom due to, e.g., switching off the mobile station MS or a low battery charging state at the mobile station's side or a removal and/or taking off a SIM card (subscriber identity module) as examples for a respective predetermined detach condition for the mobile
30 station, a detach procedure according to the present invention is performed. In particular, in this detach procedure, the mobile station MS when requesting and/or initiating detach, sends a detach request to the network NW. The detach request contains the identification TMSI and
35 the identification signature TMSI_SIG as a pair of data

00527584-072000

items. The network compares the received two data items which identify the requesting mobile station with the previously allocated one's. If the comparison yields that the received data items are identical to the previously allocated one's, the detach is performed correctly at the network side. Because no other mobile station MS except the one to which the identifier signature and corresponding identifier were previously allocated to, knows the pair of data items, it is impossible for other mobile stations to perform a malicious detach procedure.

The following description of the drawings will set out the operation of the present invention in greater detail.

Fig. 1 shows a flowchart of the registration procedure. In step S0 the registration procedure starts. In the subsequent step S1, it is checked at the mobile station MS side, whether a registration condition is present. Such a registration condition may for example be present when said mobile station newly attaches to a network NW and has initially to be registered (authenticated) at the network NW side, or when said mobile station has moved within the network NW and a location update of said mobile station MS becomes necessary. Alternatively, also a cell update in case of the terminal having moved to an extent that the previous cell has been left and a new cell was entered represents such a registration condition. Also, in third generation networks an URA (UTRAN Registration Area, UTRAN standing for "Universal Terrestrial Radio Access Network") update is possible, thus representing a registration condition in the sense of the present invention. Such an URA update may be necessary in case of third generation networks, in which a radio network controller RNC handles the location information in terms of registration areas.

Such updates become for example necessary when the mobile station has to be registered to another controlling device MSC within the network due to "excessive" moving within the network and/or in case of a request of the mobile station MS for a traffic channel assignment.

If no registration condition is present in step S1, the procedure returns to step S1 until a registration condition is present. Then, the process proceeds to step S2.

10

In step S2, the mobile station MS sends a registration request REG_REQ to the network NW, i.e. to the network controlling device, e.g. the MSC. The registration request REG_REQ is for example an attach request for initial registration of said mobile station MS as a first type radio transceiver device in said network, or a location update request for updating a previous registration of said mobile station MS in said network, or any other request which is transmitted when any of the above described further possible registration conditions is satisfied.

20

In step S3, this registration request REG_REQ is received by the network controlling device. In response to receiving said request, the network controlling device selects or determines an identification like for example TMSI for the requesting mobile station MS.

25

Moreover, in a subsequent step S4 of the described example, the network NW (network controlling device MSC) also derives an identification signature TMSI_SIG for said identification TMSI. (However, as mentioned above, the signature may also be derived by the mobile station MS itself upon receipt of a corresponding instruction from the network NW, and the signature will then have to be informed to the network NW (not represented in the figures).)

35

00627E84 072800

Both of these data items as parameters for identifying a specific mobile station MS, namely, the identification TMSI and the (separate) identification signature TMSI_SIG are allocated to the mobile station MS in a subsequent step S5.

- 5 Of course, the network NW keeps a record of the thus assigned pair of data items.

10 The data items TMSI and TMSI_SIG are allocated in a secure mode, so that a third party may not obtain a knowledge of the assigned data items. Then, in step S6 of the described example, they are transmitted from the network NW side to the mobile station MS side in order to inform the mobile station of the allocated identification TMSI and the identification signature TMSI_SIG.

- 15 Thereafter, in step S7, the registration procedure is completed.

20 Fig. 2 illustrates a flowchart of the detach procedure when a mobile station MS as a terminal is to be detached from the network it has previously been registered to.

25 The detach procedure starts in a step S8. In a subsequent step S9, at a respective mobile station MS side, it is checked whether a predetermined condition, i.e. a detach condition, of the mobile station MS is present. Such a detach condition may for example be met in case of a power off state of said mobile station MS, or in case a low battery charging state of the battery of the mobile station

30 is detected. Alternatively, a user actuated command may fulfill the detach condition, for example, if another user wishes to use the mobile station MS as a terminal equipment and an SIM module (subscriber identity module) of the new user has to be inserted. This applies also in case of

35 removal of the SIM module.

If no such detach condition as a predetermined condition is detected, the procedure loops until a corresponding condition is detected. If a detach condition is detected at the mobile station side, the mobile station MS sends a
5 detach request DET_REQ to the network NW, i.e. to the network controlling device like an MSC, step S10.

The detach request DET_REQ contains said pair of said identification TMSI and said identification signature
10 TMSI_SIG previously allocated to said mobile station MS upon registration of the mobile station to the network NW.

In particular, the detach request DET_REQ, may for example, assume a data format as shown in Fig. 3 of the drawings. As
15 roughly schematically illustrated therein, a burst transmitted from the mobile station MS to the network NW (controlling device) contains the detach request DET_REQ. The detach request contains the pair of the identification TMSI and the identification signature TMSI_SIG. Although
20 the TMSI and TMSI_SIG are illustrated as being transmitted immediately one after the other in the burst, another burst format may be adopted in that there may be provided a guard period or dummy period (not shown) between the respective data items. Alternatively, each data item could be
25 identified by a respective flag (not shown) indicating which data item is transmitted next, and transmitted prior to the respective data item. Moreover, in the latter case, the order of the specific transmitted data items would not be restricted to a specific one, but could be changed in an
30 arbitrary manner, as long as the data items could be identified at the reception side. Furthermore, the detach request could be transmitted in a form such that for example, the identification and the identification signature could be transmitted in consecutive bursts as

respective request messages which in combination result in the request as such.

In step S11, the detach request DET_REQ is received at the network NW side. In a following step S12, the received detach request DET_REQ is compared, data item per data item, i.e. separately for the identification TMSI and the identification signature TMSI_SIG, with a record of registration data of said terminal kept at the network side. The record is the record of the previously assigned pair of data items TMSI, TMSI_SIG kept at the network NW side, as mentioned above in connection with step S5, upon registration of a respective mobile station MS to the network NW.

Namely, at the network controller side a set of such records (e.g. in form of a table) of all allocated pairs of data items TMSI, TMSI_SIG for all respective mobile stations currently registered to the network is kept, and in step S12 a check is made as to whether the received pair of TMSI, TMSI_SIG is contained as a record in said set of records (table).

If the pair of data items received with the detach request message DET_REQ is not contained in said record (NO in step S12), the procedure advances to step S13. In step S13, no detach operation is performed, and all registered mobile stations remain registered to the network. Also, an authentication procedure (registration) could then be started in this case in step S13. Therefore, a malicious user sending arbitrary identifications can not terminate any call or detach any other user, since he is not enabled to send a pair of matching data items of an identification TMSI and a corresponding identification signature TMSI_SIG.

09607684-0728000

If, however, the comparison in step S12 yields that the received detach request DET_REQ contains a pair of data items TMSI, TMSI_SIG which is contained in the table of records, i.e. has previously been allocated to a mobile station upon registration, (YES in step S12) then the flow proceeds to step S14.

In step S14, a detach operation is performed, since it has been verified that the detach request DET_REQ originated from an authentic mobile station which was previously registered to the network. Thus, an immediate authentication procedure can be carried out by comparing the pair of received data item TMSI, TMSI_SIG with a record of previously allocated (assigned) data items. This assures that a detach operation is only performed for a mobile station MS as a respective terminal, if the request for detach originates from the mobile station MS itself. Hence, no malicious user can initiate a detach of arbitrary mobile stations since he can not know the pair of the identification TMSI and the corresponding signature TMSI_SIG.

Moreover, the authentication at detach is immediately effected at the network side without involving a repeated handshaking procedure with the mobile station. Thus, the authentication procedure can also be successfully performed in case the mobile station has a too low battery charging level, has been switched off, or the like.

The procedure has been described herein above mainly with reference to the temporary mobile subscriber identity TMSI being used as an identification and for deriving the signature therefor, since the TMSI is already defined in existing radio telecommunication systems and, therefore, can be advantageously be used in connection with the

present invention. Nevertheless, the present invention can also be carried out in case a new identification and corresponding signature thereof are defined, while this, however, would require additional changes to existing
5 agreed standards.

It should be understood that the above description and accompanying drawings are only intending to illustrate the present invention by way of example. Thus, the preferred
10 embodiment of the invention may vary within the scope of the attached claims.

000220-4332360

CLAIMS

1. A method for performing a detach of a terminal (MS) registered to a telecommunication network (NW) by associating an identification (TMSI) for said terminal (MS), deriving a signature (TMSI_SIG) for said identification (TMSI), and allocating a pair consisting of said identification (TMSI) and said signature (TMSI_SIG) to said terminal (MS),
- 10 said method comprising the steps of:
- sending a detach request (DET_REQ) including said identification (TMSI) and said identification signature (TMSI_SIG) from said registered terminal (MS) to said network (NW);
- 15 receiving said detach request (DET_REQ) at the network (NW) side;
- comparing said received detach request (DET_REQ) with a record of registration data of said terminal (MS) kept at the network side; and
- 20 detaching said terminal (MS) from said network (NW), if said received detach request (DET_REQ) coincides with said record of registration data.
2. A method according to claim 1, wherein,
- 25 sending of said detach request message (DET_REQ) is initiated upon detection of a predetermined state of said terminal (MS).
3. A method according to claim 2, wherein
- 30 said predetermined state is a power off state.
4. A method according to claim 2, wherein
- said predetermined state is a low battery state.
- 35 5. A method according to claim 2, wherein

said predetermined state resides in a removal of a SIM module from said terminal.

6. A method according to claim 1, wherein

5 said record of registration data contains said pair
consisting of said identification (TMSI) and said
identification signature (TMSI_SIG), and

said comparison is effected for each of said data items forming said pair.

7. A method according to claim 1, wherein

said identification (TMSI) is the temporary mobile subscriber identity.

15 8. A method according to claim 1, wherein

said identification is the international mobile subscriber identity IMSI.

9. A method for registration of a terminal (MS) to a telecommunication network (NW),

said method comprising the steps of:

associating an identification (TMSI) for said terminal (MS),

deriving a signature (TMSI SIG) for said

25 identification (TMSI), and

allocating a pair consisting of said identification (TMSI) and said signature (TMSI_SIG) to said terminal (MS).

10. A method according to claim 9, further comprising the
30 step of

sending a registration request (REG_REQ) from said terminal (MS) to said network (NW); and wherein

said associating is effected in response to the receipt of said registration request.

[illegible]

11. A method according to claim 10, wherein
 said registration request (REG_REQ) is an attach
 request for initial registration of said terminal (MS) in
 said network (NW).

5

12. A method according to claim 10, wherein
 said registration request (REG_REQ) is a location
 update request for updating a previous registration of said
 terminal (MS) in said network (NW).

10

13. A method according to claim 10, wherein
said registration request (REG_REQ) is a-cell update
request for updating a previous registration of said
terminal (MS) in said network (NW).

15

14. A method according to claim 10, wherein
 said registration request (REG_REQ) is a URA update
 request for updating a previous registration of said
 terminal (MS) in said network (NW).

20

15. A method according to claim 9, wherein
said associating of said identification (TMSI) is
arbitrary.

25

16. A method according to claim 9, wherein
said allocating is effected in a secure mode.

30

17. A method according to claim 9, wherein
said identification (TMSI) is the temporary mobile
subscriber identity.

18. A method according to claim 9, wherein
said identification is the international mobile
subscriber identity IMSI.

35

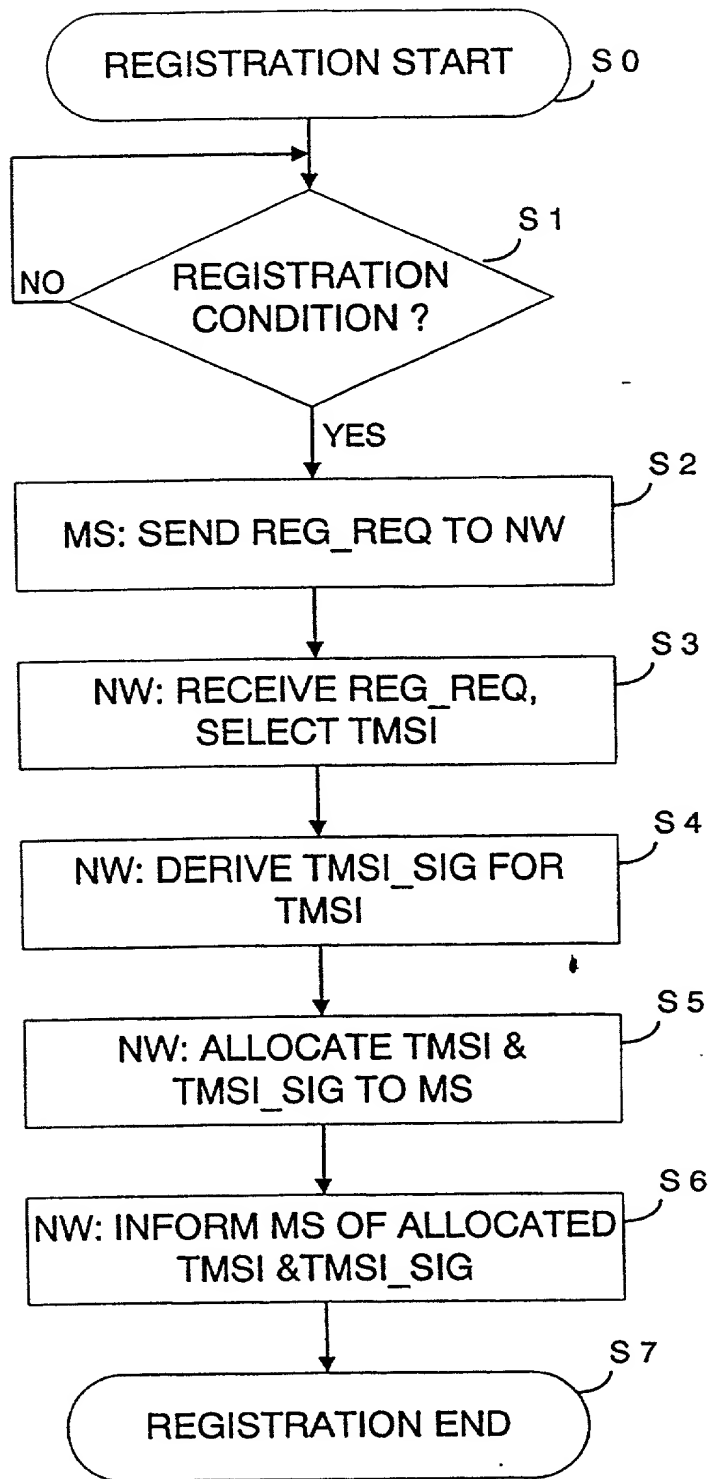
19. A terminal device adapted to the method according to any of claims 1 to 18.

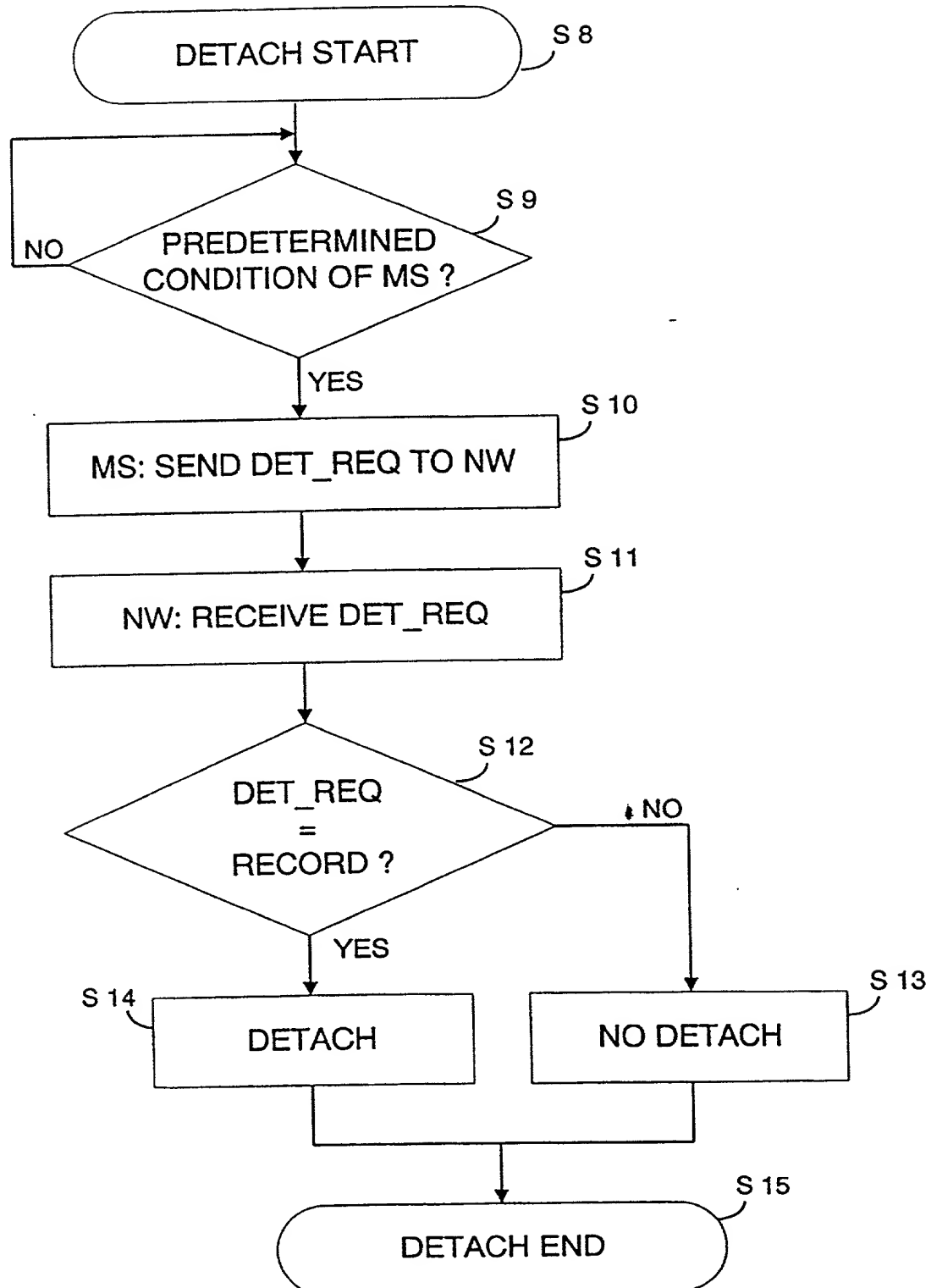
20. A network controlling device adapted to the method
5 according to any of claims 1 to 18.

21. A telecommunication system consisting of at least one terminal (MS) and at least one network controlling device controlling at least one radio transceiver device, adapted to carry out the method according to any of claims 1 to 18.

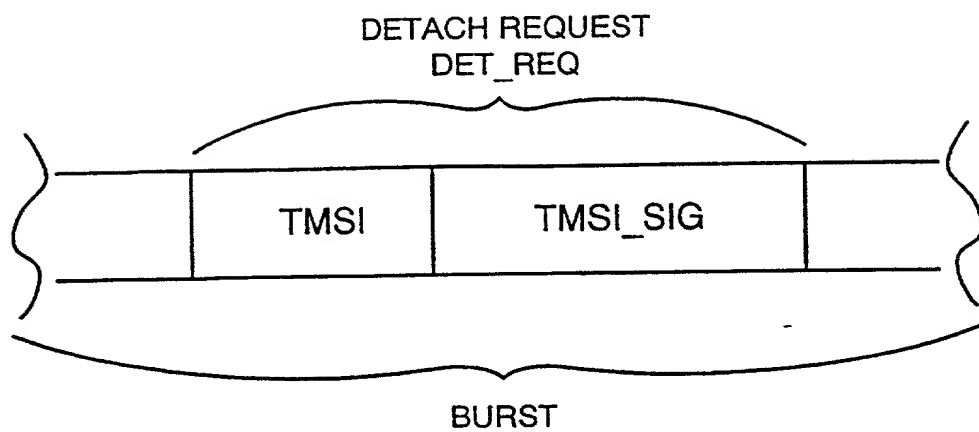
THE 1990S

The present invention proposes a method for performing a detach of a terminal (MS) registered to a telecommunication network (NW) by associating an identification (TMSI) for said terminal (MS), deriving a signature (TMSI_SIG) for said identification (TMSI), and allocating a pair consisting of said identification (TMSI) and said signature (TMSI_SIG) to said terminal (MS), said method comprising the steps of: sending a detach request (DET_REQ) including said identification (TMSI) and said identification signature (TMSI_SIG) from said registered terminal (MS) to said network (NW); receiving said detach request (DET_REQ) at the network (NW) side; comparing said received detach request (DET_REQ) with a record of registration data of said terminal (MS) kept at the network side; and detaching said terminal (MS) from said network (NW), if said received detach request (DET_REQ) coincides with said record of registration data. Also, the present invention relates to a corresponding registration method and proposes a new format for a detach request message transmitted from a mobile station (MS) as a terminal to a network (NW) controlling device like an MSC, and also relates to correspondingly adapted devices.

1/3
FIG. 1

2/3
FIG. 2

3/3
FIG. 3



09627634, 072200

Altera Law Group, LLC

**Declaration and Power of Attorney Patent Application
(Design or Utility)**

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name,

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled: A METHOD FOR A SECURE DETACH PROCEDURE IN A RADIO TELECOMMUNICATION NETWORK

the specification of which

- ☐ is referred to by Altera reference number on a separate document
☒ is attached hereto
☐ was filed on _____ as application serial no. _____ and or PCT International Application number _____ and was amended on _____ (if applicable).

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose to the U.S. Patent and Trademark Office all information know to me to be material to patentability as defined in 37 C.F.R. §1.56.

I hereby claim foreign priority benefits under 35 U.S.C. §119(a)-(d) or 35 U.S.C. §365(b) of any foreign application(s) for patent or inventor's certificate, or 35 U.S.C. §365(a) of any PCT International application which designated at least one country other than the United States, listed below and have also identified below any foreign application for patent or inventor's certificate of PCT International application having a filing date before that of the application on which priority is claimed.

Prior Foreign Application(s)		
Number	Country	Day/Month/Year Filed
Number	Country	Day/Month/Year Filed
Number	Country	Day/Month/Year Filed

I hereby claim the benefit under 35 U.S.C. §119(e) of any United States provisional application(s) listed below:

Prior Provisional Application(s)	
Serial Number	Day/Month/Year Filing Date
Serial Number	Day/Month/Year Filing Date
Serial Number	Day/Month/Year Filing Date

I hereby claim the benefit under 35 U.S.C. §120 of any United States application(s), or under 35 U.S.C. §365(c) of any PCT International application designating the United States, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT International application in the manner provided by the first paragraph of 35 U.S.C. §112, I acknowledge the duty to disclose to the U.S. Patent and Trademark Office all information known to me to be material to patentability as defined in 37 C.F.R. §1.56 which became available between the filing date of the prior application and the national or PCT International filing date of this application:

Prior U.S. or International Application(s)		
Serial Number PCT/EP98/08064	Day/Month/Year Filed 10 December 1998	Status (patented, pending, abandoned) Pending
Serial Number	Day/Month/Year Filed	Status (patented, pending, abandoned)
Serial Number	Day/Month/Year Filed	Status (patented, pending, abandoned)

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements are made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under 18 U.S.C. §1001 and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Power of Attorney

As a named inventor, I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith.

Steven R. Funk Reg. No. 37,830
David W. Lynch Reg. No. 36,204
Karen D. McDaniel Reg. No. 37,674

Mark A. Hollingsworth Reg. No. 38,491
Michael B. Lasky Reg. No. 29,555
Iain A. McIntyre Reg. No. 40,337

I hereby authorize them or others whom they may appoint to act and rely on instructions from and communicate directly with the person/organization who/which first sends this case to them and by whom/which I hereby declare that I have consented after full disclosure to be represented unless/until I instruct Altera Law Group, LLC otherwise.

Please direct all correspondence in this case to Altera Law Group, LLC at the address indicated below:

Michael B. Lasky
Altera Law Group, LLC
10749 Bren Road East, Opus 2
Minneapolis, MN 55343

Full Name of Sole or First Inventor		
Family Name Rajaniemi	First Given Name Jaakko	Second Given Name
Residence and Citizenship		
City of Residence Helsinki	State or Country of Residence Finland	Country of Citizenship Finland
Post Office Address		
Street Address Lapinrinne 2 A 11	City 00180 Helsinki 18	State & Zip Code or Country Finland
Signature of Inventor		Date